We claim:

1. A digital signature generation method for generating a digital signature for electronic information existing on a storage unit of a terminal in a system configured to enable said terminal and a server device to communicate with each other via a network, said method comprising steps of:

calculating, in said terminal, a Digest value for the electronic information;

sending, from said terminal to said server device, the Digest value and identifying information of a user as an issuer of the electronic information;

taking, in said server device, a secret key corresponding to the identifying information received from said terminal, out of a storage device stored with a pair of a secret key and a public key related with identifying information of each user;

generating, in said server device, a signature value by encrypting the Digest value received from said terminal with the secret key taken out of said storage device;

responding, from said server device to said terminal, the generated signature value; and

forming, in said terminal, undersigned electronic information by attaching the signature value and the identifying information responded from said server device to the electronic information.

2. A digital signature authentication method for authentication undersigned electronic information obtained by said digital signature generation method according to claim 1, in a system configured to enable said terminal and a server device to communicate with each other via a network, said method comprising steps of:

calculating, in said terminal, a Digest value for electronic information in the undersigned electronic information;

sending, from said terminal to said server device, the Digest value, and a signature value and the identifying information in the undersigned electronic information;

taking, in said server device, a public key corresponding to the identifying information received from said terminal, out of said storage device;

decrypting, in said server device, the signature value received from said terminal with the public key taken out of said storage device;

comparing, in said server device, a substance of the decrypted signature value with the Digest value received from said terminal; and

responding, by said server device, a result of the comparison to said terminal.

3. A digital signature generation request program for a computer communicable via a network with a server device including a storage device stored with a pair of a secret key and a public key related with identifying information of each user, said computer taking, when receiving a digital signature generation request message designating encryption object information and identifying information, the secret key corresponding to the received identifying information out of said storage device, generating a signature value by encrypting the encryption object information with the secret key and responding the generated signature value, said program making said computer:

(a) if electronic information and identifying information of a user as an issuer of the electronic information are specified,

calculate a Digest value for the electronic information; and

send the digital signature generation request message containing the calculated Digest value as the encryption object information and the identifying information to said server device; and

(b) if the signature value is responded from said server device,

form undersigned electronic information by attaching the signature value and the identifying information to the electronic information.

4. A digital signature authentication request program for a computer communicable via a network with a server device including a storage device for stored with a pair of a secret key and a public key related with identifying information of each user, said computer taking, when receiving a digital signature authentication request message designating authentication object information, signature value and identifying information, the public key corresponding to the received identifying information out of said storage device, decrypting the signature value with the public key, comparing the decrypted signature value with the authentication object information, and responding a result of the comparison, said program making said computer:

if undersigned electronic information obtained according to claim 1 or 3 is inputted,

calculate a Digest value for the electronic information in the undersigned electronic information; and

send the digital signature authentication request message containing the Digest value as the authentication object information and the signature value and the identifying information in the undersigned electronic information to said server device.